IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Special Issue 1, April 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Management of Data Security in Cloud Computing Using Hybrid Encryption

[1]Muttappa Mantur, [2]Dr. Amit Jain

[1]Research Scholar, Department of Computer Science and Engineering, SunRise University, Alwar, Rajasthan, India

[2]Research Supervisor, Department of Computer Science and Engineering, SunRise University, Alwar, Rajasthan, India

ABSTRACT: Cloud computing has enhanced the focus on accessing and storing data. Sharing and storing information through the cloud plays a key role in providing users with cost-effective, flexible and reliable solutions. Despite the benefits of cloud-based systems, data security is a major factor limiting the adoption of cloud-based models. Everyone needs to protect their data or information from theft or corruption. The use of encryption algorithms helps solve the problem of data protection in cloud storage. Encryption plays a key role in achieving the level of security required for cloud. Therefore, this study describes managing data security in cloud computing using hybrid cryptography. The primary purpose of this analysis is to provide hybrid security model that produces security for cloud storage. Hybrid encryption utilizes the integration of multiple encryption algorithms to improve overall security and performance. This approach uses a combination of SHA-256 and ciphertext policy attribute-based encryption (CP-ABE), uses SHA-256 to compute hash value, and uses CP-ABE to store cloud Encrypt your data. This approach yields better results in terms of encryption time, decryption time, confidentiality, integrity, throughput and reliability.

KEYWORDS: Cloud computing, security of data, data storage, cryptography, encryption techniques.

I.INTRODUCTION

Cloud computing is gaining popularity as an emerging technology for sharing the resources over the Internet. Cloud computing provides flexibility, reliability, sustainability and cost effectiveness to the users. Nowadays cloud computing is widely used because of its easy access and high-level security and availability. Cloud computing is even more affordable for storing and accessing the information.

Day to day use of cloud data is increasing because of access in two gatherings but its challenging to give security as well as privacy to increased users for cloud use. In cloud computing data must be secure at all stages like while storing, while processing and also while uploading the data. The majority of corporations are transitioning from traditional data storage to cloud storage, which provides an efficient way to access data anywhere, at any time.

Cloud computing provides cloud services online. The Cloud computing model allows apps once information is accessed remotely. Three levels of services used are d to define as cloud computing infrastructure as a service (IaaS), Software as a service (SaaS), and Platform as a Service (PaaS). IaaS provides visual equipment and storage to users. SaaS provides users with frameworks to improve cloud hosting applications to develop, use, analyze, and manage theorem services. PaaS provides users with services and applications with a web browser anywhere at any time and any place [5].

However, one of the major challenges in implementing cloud computing for businesses is data security. These attackers may be internal (Cloud Service Provider) or external. Since, Cloud Computing has various technologies; it is prone to the security issues of those technologies as well. These technologies include databases, virtualization, resource scheduling, operating systems, concurrency control, networks, transaction management, and memory management. Therefore, data security is a primary concern, so proper enforcements should be done regarding to it [6].

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Data is considered the most important thing these days. Information security is the major issue in technology development, and it seems to be the most critical and necessary to maintain data privacy while transmitting through the network. The data of users and business organizations lies together on a platform that can be accessed by anyone as they provide control to a third party over their data. So, it is at a risk of being accessed by someone who is not authorized. Thus leading to breach in data. More generally, cryptography is about building and analyzing protocols, which prevent private messages from being read by third parties or the public [3].

Cloud storage is a way that allows you to store your data on hosted server. When different organizations use the cloud to store their data, the chances of data misuse increases. To avoid this kind of situations there is an imminent need to secure the data. Also, the data needs to be protected from unauthorized access. Security is very important feature for any technology. Using any technology will not be worth if it is not secure This Security concern of protecting the data from unauthorized access can be solved using various ways, the most commonly used techniques are cryptography [4].

Cryptography contains three categories: secret key (symmetric) cryptographic public-key key (asymmetric) cryptography, as well as hash functions. Public key encryption is referred to as symmetric key exchange in the middle of the transmitter as well as the receiver of data. In Asymmetric key cryptography, public key encryption is a kind of encryption that employs two distinct keys, one for encryption (public key) and decryption (private key) [1].

Symmetric encryptions, such as (DES, RC2, RC4, Blowfish, RC5, RC6, or AES) are the oldest and method of encryption in which only a single secret key is used to encrypt and decrypt data. The sender and receiver share the key, which is a major drawback because the key exchange channel can be searched by an intruder to decrypt the data. To turn the secret key you need a secure channel between the sender and receiver. In comparison, asymmetric encryption, like DSA, RSA and ECC, uses two keys for plain text ciphering, both public and private. Any entity with a public key can use it to send a message but the private key is kept secret and used to decrypt the message. Both symmetric and asymmetric ciphers have benefits and limitations. Symmetric ciphers are fast but suffer key exchanging. Asymmetric ciphers solve the key exchange problem but slow [2].

Cloud Computing is the most emerging technologies in the world. Security is also very important in Cloud. Though there are no security issues in the cloud, still there is lack of security in the cloud. The need for cloud storage grows day after day due to its reliable and scalable nature. The storage and maintenance of user data at a remote location are severe issues due to the difficulty of ensuring data privacy and confidentiality [8]. Many researchers have presented different encryption techniques, hybrid techniques to solve these issues, however still there is no particular system to manage cloud data security. It is essential to design a effective cloud storage data security.

In order to fulfill this, Management of data security in cloud computing using hybrid encryption is presented. The Attribute-based access control provides the flexibility of the method that supports data owners to combine data access policies within the encrypted data. The sharing of cloud resources by different types of users can be easily done through this service and enhance the capability of the system by securing more storage after the implementation of the presented approach.

The rest of the work is organized as follows: The Literature survey is discussed in section II. The section III describes the Management of data security in cloud computing using hybrid encryption. The section Iv evaluate the result analysis of presented approach. Finally, the conclusion is presented in section V.

II. LITERATURE SURVEY

Srinivasan Thiruvengadam, Dr. Ramalingam sugumar et. al., [7] describes Hybrid Encryption Technology for Secure File Storage in Cloud Computing. A new security technique is introduced on symmetric key cryptography and Steganography. Rivest cipher 6 (RC6), Advanced Encryption Standard (AES), Byte Rotation Algorithm (BRA) and blowfish techniques to provide block safety information and the length of the technical key was 128 bits. A critical data security, Least Signification Bit (LSB) Steganography algorithm was applied. A document was allocated to eight

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

sections. The multiprocessing method secures all of the document's sections at the same moment. Data encryption keys were built into the primary image using the LSB technique. Steganography image was emailed to an appropriate recipient. The Reverse Cryptography procedure should be used for document decoding. This proposed method gives more security to data, documents or files during the multi-processor.

Sherief H. Murad and Kamel H. Rahouma et. al., [10] describes Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment. In this research, authors have presented a comparative study for two-tier versus three-tier hybrid cryptographic models applied to secure data on the cloud. Practical implementation was made to the studied hybrid models using python simulation. Finally, a performance analysis was conducted in terms of encryption time, decryption time, average throughput, and efficiency using relatively larger data files. According to the experimental results, we observed the superiority of the Advanced Encryption Standard (AES) hybrid model among the other algorithms in terms of performance. Also, they found that the two-tier hybrid cryptographic model is more efficient than the three-tier model, but the latter provides more security.

Dr. B. Arputhamary, A. Benita et. al., [12] describes Hybrid Encryption of Big Data Security Using Improved Elliptic Curve Cryptography. Hybrid cryptographic technique is proposed in this paper to enhance data protection during network transmission, and its implementation and results are published. The proposed secure cryptographic technique promises to use the Enhanced ECC and AES technologies to include the highly secure cypher generation technique. Using JAVA technology, the implementation of the proposed technique is given and its efficiency in terms of space and time complexity is calculated and compared with conventional ECC cryptography. During comparative performance analysis, the proposed cryptographic technique established the successful and enhanced cypher text.

Nadesh R.K, Srinivasa Perumal R, Shynu P.G and Gaurav Sharma et. al., [16] describes Enhancing security for end users in cloud computing environment using hybrid encryption technique. The proposed system will provide client level security using hybrid encryption techniques. Using AES (Advance Encryption Standard) in CBC Mode (Cipher Block Chaining) and HMAC-SHA-1 (Hash-based Message Authentication Code) with light weight methods enhances the strong encryption at client level security. Fusion of these algorithms adds extra layers of security to the cloud storage data. The proposed method enhances the security measures for any client users, using storage as a service offered by several cloud service providers.

Nivedita Shimbre, Priya Deshpande et. al., [18] describes Enhancing Distributed Data Storage Security for Cloud Computing Using TPA (Third Party Administrator) and AES algorithm Also availability is a major concern on cloud. This paper, discusses the file distribution and SHA-1 technique. When file is distributed then data is also segregated into many servers. So here the need of data security arises. Every block of file contains its own hash code, using hash code which will enhance user authentication process, only authorized person can access the data. Here, the data is encrypted using advanced encryption standard, so data is successfully and securely stored on cloud. Third party auditor is used for public auditing. This paper discusses the handling of some security issues like Fast error localization, data integrity, data security. The proposed design allows users to audit the data with lightweight communication and computation cost. Analysis shows that proposed system is highly efficient against malicious data modification attack and server colluding attack.

Navdeep Singh and Pankaj Deep Kaur et. al., [20] describes A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks. In this approach, a hybrid technique is proposed using two different techniques to provide the security to data on the higher level. This technique is beneficial in simple data transfer and storing the data on cloud. Some experimental analysis has been done on the basis of performance, execution time, response time and the CPU performance in VM telemetry view. Concluding all the different parameters the response time is low and performance of proposed technique is higher than the other two techniques and it is providing the higher security to the data. But only one drawback here is the execution time. The time taken to execute the whole process is higher than the other two techniques.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

III. MANAGEMENT OF DATA SECURITY IN CLOUD COMPUTING

In this work, Management of data security in cloud computing using hybrid encryption is presented. The Fig. 1 shows the workflow of Management of data security in cloud computing using hybrid encryption.

The main aim of this work is to secure confidential data by encrypting, converting the data into binary form and storing it on the cloud. Cloud computing is a promising technology which helps organizations expand and safely transfer data from physical locations to the 'cloud' server that can be accessed from anywhere at any time. Different characteristics of cloud computing provides services to the users irrespective of their type.

The architecture consist of set of users, Cloud service providers and authorities and general users and it is contains the following modules. The sensor nodes monitor and collect the user data in regular intervals. User need to register first by filling up basic registration details. By using the login id and password, user can login into the system. Login data has the information of all the details of admin and users whereas data collection has the information of uploaded files like id, user type, public keys, edata, file name and time. Login details include user name, password and type. The cloud service providers access the stored data using the monitoring applications.

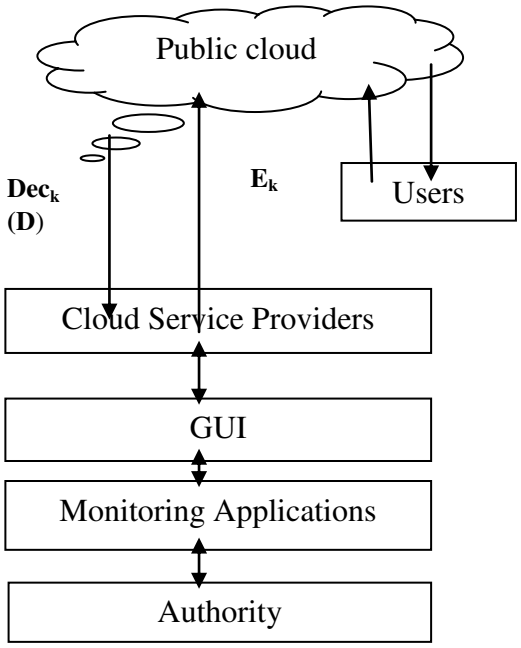

Fig. 1: Workflow diagram of Management of data security in cloud computing using hybrid encryption

A CSP (cloud service provider) is a third-party company that provides scalable computing resources that businesses can access on demand over a network, including cloud-based compute, storage, platform, and application services. Cloud service providers are companies that establish public clouds, manage private clouds, or offer on-demand cloud computing components. The graphical user interface, or GUI, is a form of user interface that allows users to interact with electronic devices through graphical icons and visual indicators.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

The Cloud Authority (CA) is responsible for security policies of the organizations and users. The cloud storage is used for storing the data and also preserves the data security. Each sensor node forwards the sensed data to the gateway where the data aggregation is performed along with the encryption using the Randomly generated Symmetric key (RSk). The encrypted data is stored in the cloud. The cloud service providers use monitoring applications to supervise the user data from any location. The cloud authority download the data from the cloud and decrypts using the secret key. The monitoring applications use RSK for data encryption and uses CA for access privileges. The sensor nodes monitor and record the user data and forward the collected data to a central location.

The Secure Sockets Layer (SSL) protocol was developed by Netscape Communications Corporation. SSL ensures the data that is transferred between a client and a server remains private. This protocol enables the client to authenticate the identity of the server.At the initial stage, Cloud Authority (CA) attribute set and uses ABE algorithm for generating the public key (PU_k) and the master key (M_k). Attribute-based encryption (ABE) can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes. An attribute based encryption scheme (ABE), in contrast, is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each ciphertext.

The public key (PU_k) is disclosed to all the users and it is used to encrypt and decrypt the data. The master key (M_k) is kept secret from the users. To disclose the PU_k, the CA ciphers it with the private key (PR_k) and forwards to the cloud service providers (CSP). The user downloads the PU_k and validates the authenticity. Users can join and leave the network at any time. If the new user has to join in to the network, The CA has to assign the secret key (S_k) along with the access privileges to the new user. The access privileges (A_P) provides the flexibility to the new user to encrypt and decrypt the data before sending to the cloud.

Firstly, the PKI (Public Key Infrastructure) generates public key, private key (PU_k, PR_k) to the user, then CA uses CP-ABE algorithm for generating the secret (S_k) and A_P to the user. CA requests the cloud to add the user identification (U_{Id}) to the user list (Lu). After receiving the request from the CA, the cloud adds U_{Id} along with its PUk to the user list (Lu). Once the user gateway creates the communication with the CA, then the user receives the S_k, A_P and PR_k. The security parameters of the CSP and the users requirements are different. The user needs to encrypt the health data before sending in to the cloud and it is in read only mode. The user data send by the cloud need to be encrypted and it is in both read (R) and write mode (W). CA provides the access privileges of users and CSPs in different methods.

The access privileges of cloud are composed of two parts: one is for encrypting the data and another one is for write mode protection. The data is collected by the sensor nodes and the data is accessed only in the read mode. The sensor nodes continuously send the sensed data to the gateway G. U_{Id} forwards the userdata to the gateway. The gateway G generates the RS_k using the symmetric key encryption algorithm, then compute the hash value using SHA-256 algorithm.

The SHA-256 algorithm is a widely used hash function with 256 bit hash value. SHA-256 stands for Secure Hash Algorithm 256-bit and it's used for cryptographic security. Cryptographic hash algorithms produce irreversible and unique hashes. The larger the number of possible hashes, the smaller the chance that two values will create the same hash. SHA-256 generates almost unique 32 bit hash. With recent computational advancements, it has become possible to decrypt SHA-256 hashes. Much stronger than SHA-1, it includes the most secure hashing algorithm available to the time of writing. Then, G encrypts the user data (D) and Hash value (H) using the RS_k and adds the access privileges to the encrypted RS_k and finally forwards the encrypted clouud data $\{U_{Id}, E_k \{RS_k, A_p\}, E_k (D+H)RS_k\}$ to the cloud service provider CSP.

After the gateway transmits the encrypted data to the CSP, the users can access the data and decrypts it by submitting the secret key S_k. The user has to perform the
additional step of validating the RS_k with CP-ABE algorithm. A ciphertext-policy attribute based encryption scheme consists of four algorithms: Setup, Encrypt, KeyGen, and Decrypt. In the Ciphertext-Policy Attribute-Based Encryption

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

model, the data owner encrypts data using an attribute-based access structure before sending them to the storage service, and only users with authorized sets of attributes can successfully decrypt the generated cipher-text.

After decrypting, the user has to validate the data integrity. If any discrepancies are noticed in the decrypted data, the user has to send the message to the CA. To access the uploaded file, one must have the private key and not just the public key. To download the file one must have the name and private key of that respective file. Using them the actual file can be downloaded. The information is kept in a database to which only the admin has access. Database contains the data of login and uploaded files.

The user data consist of user personal details, images, passwords, Transaction details, Bank account details, etc. This data can be modified by any other users who are having the write access. However, to restrict write access, the password is provided for each file. If any user has to perform the write operation on the file, they need to submit the password of the specific file. If the password is not matched then file/data access will be denied.

IV. RESULT ANALYSIS

In this section, Management of data security in cloud computing using hybrid encryption is implemented. In this approach, the combination of SHA-256 and CP-ABE is used as Hybrid Encryption model. User data files are encrypted using the symmetric key and CP-ABE is used for encrypting the symmetric key. The CP-ABE algorithm is efficient against the unauthorized access. The performance of this hybrid encryption is evaluated here in terms of Encryption Time, decryption time, Confidentiality, Integrity, Throughput and Authenticity and are defined as follows:

Throughput: Throughput is the amount of the work a computer can do in a given period of time. It is a measure of comparative effectiveness of large computers that run programs concurrently.

Encryption Time: The time required to encrypt data is termed as encryption time of the cryptographic system.

Decryption time: The time to recover original data from cipher is known as decryption time.

Data confidentiality refers to protection of data from unauthorized access and disclosure, including means for protecting personal privacy and proprietary information.

Authenticity: It is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

Integrity: Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

The Fig. 2 shows the Encryption time comparison. In Fig. 2, the x-axis indicates the file size in terms of Mega Bytes (MB) and y-axis represents the encryption time in terms of seconds (s). From Fig. 2 it is clear that the encryption time is increasing as the size of the file is increases. The encryption performance of presented hybrid encryption approach is compared with secure file storage using Hybrid cryptography. However, compared to earlier hybrid cryptography approach, presented hybrid encryption approach has better encryption time i.e. it requires less time for encryption.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

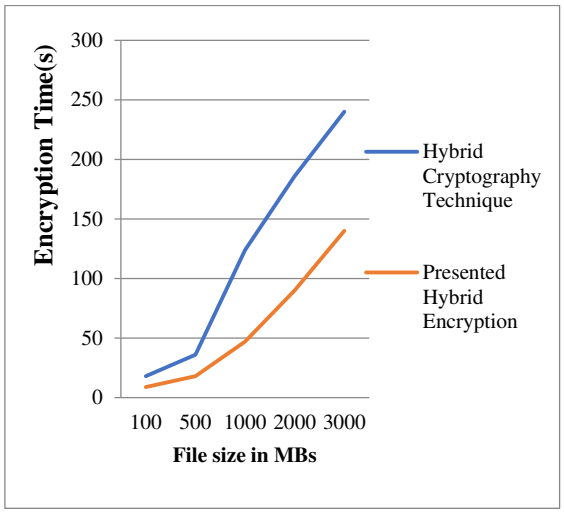

Fig. 2: Encryption Time Comparison

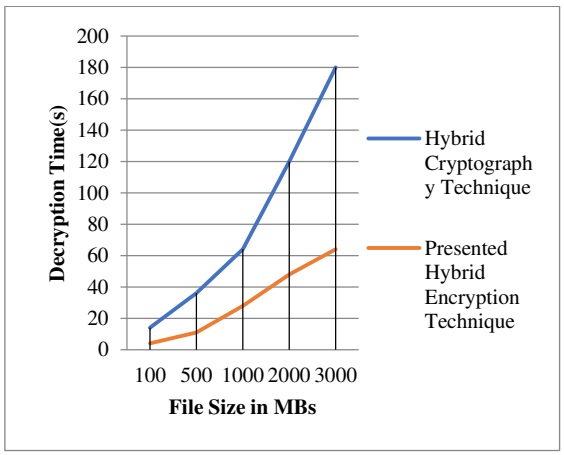

Fig. 3: Decryption Time Comparison

The Fig. 3 shows the decryption time. In Fig. 3, the x-axis indicates the file size in terms of Mega Bytes (MB) and y-axis represents the decryption time in terms of seconds (s).

Presented hybrid encryption model has required very less decryption time than earlier hybrid cryptography technique. The Fig. 4 shows the Throughput performance comparison. In Fig. 4, the x-axis indicates different approaches and y-axis indicates the throughput in terms of kb/seconds (kilo Bytes per second).

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

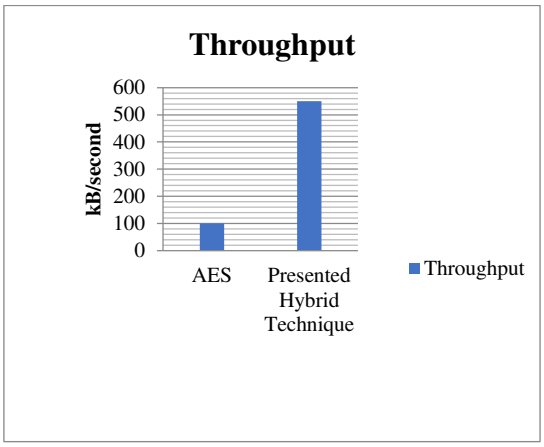

Fig. 4: Throughput Comparison

Compared to AES Approach, Presented approach has better throughput. The Table 1 shows the performance comparison.

Table 1: Performance Comparison

Parameters/Methods	AES Algorithm	Management of data security in cloud computing using hybrid encryption
Integrity (%)	80	97.83
Confidentiality (%)	85.63	98.25
Authenticity (%)	84.21	98.45

The performance of presented hybrid encryption is measured in terms of Integrity, Confidentiality and Authenticity. Presented Hybrid Encryption has better performance. The Fig. 4 represents the graphical representation of performance comparison.

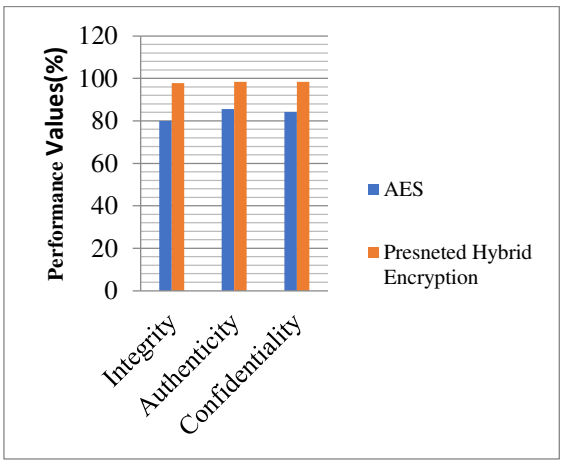

Fig. 5: Performance Comparison

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

From the figure, it is observed that, Hybrid encryption has shown significant results in terms of authenticity, integrity and confidentiality compared to AES Approach. From the results, it is proved that random secret key and Hybrid encryption ensures the confidentiality and guarantees the security of the stored data.

V. CONCLUSION

Cloud computing is a location-independent environment that shares calculations and resources to provide high-performance services The majority of consumers and businesses are shifting to the cloud since it is considerably cheaper and more convenient. Ensuring the security of cloud computing is one of the most critical challenges facing the cloud services sector. Dealing with data in a cloud environment, which uses shared resources, and providing reliable and secure cloud services, requires a robust encryption solution with no or low negative impact on performance. To solve these issues, Management of data security in cloud computing using hybrid encryption is presented in this work. The hybrid model is developed while combining the efficient access control mechanism by combining the SHA-256 and Cipher text Policy-Attribute Based Encryption (CP-ABE). This Architecture is presented for managing the large volumes of cloud data of users. This approach is an efficient architecture that uses cloud environment to store the data dynamically. This security model avoids the security issues of cloud data and provides the confidentiality, integrity with any user interventions. This hybrid algorithm reduced encryption and decryption time. Performance of presented hybrid encryption approach is measured in terms of throughput, confidentiality, integrity and authenticity. Compared to earlier approaches, presented approach has better and significant results.

REFERENCES

[1] Abel Yeboah-Ofori, Christian Kwame Agbodza, Francisca Afua Opoku-Boateng, Iman Darvishi, Fatim Sbai, "Applied Cryptography in Network Systems Security for Cyberattack Prevention", 2021 International Conference on Cyber Security and Internet of Things (ICSIoT), DOI: 10.1109/ICSIoT55070.2021.00017

[2] Reece B. D'Souza, Yash Priyadarshi, "Improving Security of IoT Devices using Cryptographic Algorithms", International Research Journal of Engineering and Technology (IRJET), Volume: 08 Issue: 11, Nov 2021, e-ISSN: 2395-0056

[3] Karthick Raj V K, Rajarajeswari P, "A Scalable Cryptography Policies For Secure Data Storage And Access The Data In Cloud Environment", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 08 Issue: 02, Feb 2021

[4] Akash Phad, Abhijit Shinde, Akshay Lukaday, Suraj Chandugade, Nikhilkumar Shardoor, "Framework on Secure File Repository in Cloud using Hybrid Cryptography Techniques", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 08 Issue: 07, July 2021,

[5] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient Data Security Using Hybrid Cryptography on Cloud Computing", Inventive Communication and Computational Technologies, Lecture Notes in Networks and Systems 145, Springer, 2021, doi: 10.1007/978-981-15-7345-3_46

[6] Sanjeev Kumar, Garima Karnani, Madhu Sharma Gaur, Anju Mishra, "Cloud Security using Hybrid Cryptography Algorithms", 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), DOI: 10.1109/ICIEM51511.2021.9445377

[7] Srinivasan Thiruvengadam, Dr. Ramalingam sugumar, "Hybrid Encryption Technology for Secure File Storage in Cloud Computing", International Journal of Computational Intelligence in Control,
Vol.13 No. 2 December, 2021,

[8] Noha E. El-Attar, Doaa S. El-Morshedy and Wael A. Awad, "A New Hybrid Automated Security Framework to Cloud Storage System", Cryptography 2021, 5, 37. doi:10.3390/cryptography5040037

[9] Saba Rehman, Nida Talat Bajwa, Munam Ali Shah, Ahmad O. Aseeri and Adeel Anjum, "Hybrid AES-ECC Model for the Security of Data over Cloud Storage", Electronics 2021, 10, 2673, doi:10.3390/electronics10212673

[10] Sherief H. Murad and Kamel H. Rahouma, "Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment", 18th International Learning & Technology Conference 2021, doi: 10.1016/j.procs.2021.10.070

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 11, Special Issue 1, April 2022*

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

[11] Hossein Abroshan, "A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms",
(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 6, 2021
[12] Dr. B. Arputhamary, A. Benita, "Hybrid Encryption Of Big Data Security Using Improved Elliptic Curve Cryptography", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 9, Issue. 10, October 2020, pg.83 – 94
[13] Mustafa S. Abbas, Suadad S. Mahdi, Shahad A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography", 2020 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Kurdistan Region – Iraq, 978-1-7281-5249-3/20
[14] Yoshita Sharma, Himanshu Gupta; Sunil Kumar Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing", 2019 Amity International Conference on Artificial Intelligence (AICAI), DOI: 10.1109/AICAI.2019.8701398
[15] Vanaja Malgari, Raman Dugyala, Ashwani Kumar, "A Novel Data Security Framework in Distributed Cloud Computing", 2019 Fifth International Conference on Image Information Processing (ICIIP), 2019 IEEE.
[16] Nadesh R.K, Srinivasa Perumal R, Shynu P.G and Gaurav Sharma, "Enhancing security for end users in cloud computing environment using hybrid encryption technique", International Journal of Engineering & Technology, 7 (1) (2018) 152-156, doi: 10.14419/ijet.v7i1.8340
[17] Punam V. Maitri, Aruna Verma, "Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm", 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), DOI: 10.1109/WiSPNET.2016.7566416
[18] Nivedita Shimbre, Priya Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm", 2015 International Conference on Computing Communication Control and Automation, DOI 10.1109/ICCUBEA.2015.16
[19] Niteen Surv, Balu Wanve, Rahul Kamble, Sachin Patil, Jayshree Katti, "Framework for client side AES encryption technique in cloud computing", 2015 IEEE International Advance Computing Conference (IACC), DOI: 10.1109/IADCC.2015.7154763
[20] Navdeep Singh and Pankaj Deep Kaur, "A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks", International Journal of Database Theory and Application Vol.8, No.3 (2015), pp.145-154,doi:10.14257/ijdta.2015.8.3.12

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details